

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-204998

(43)公開日 平成6年(1994)7月22日

(51)Int.Cl.⁵

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/00

9/10

9/12

7117-5K

8732-5K

H 0 4 L 9/ 00

11/ 26

Z

審査請求 未請求 請求項の数19(全 12 頁) 最終頁に続く

(21)出願番号 特願平5-237161

(22)出願日 平成5年(1993)8月31日

(31)優先権主張番号 9 3 7 0 0 9

(32)優先日 1992年8月31日

(33)優先権主張国 米国(US)

(71)出願人 390035493

アメリカン テレフォン アンド テレグ
ラフ カムパニー

AMERICAN TELEPHONE
AND TELEGRAPH COMPA
NY

アメリカ合衆国 10013-2412 ニューヨ
ーク ニューヨーク アヴェニュー オブ
ジ アメリカズ 32

(74)代理人 弁理士 三俣 弘文

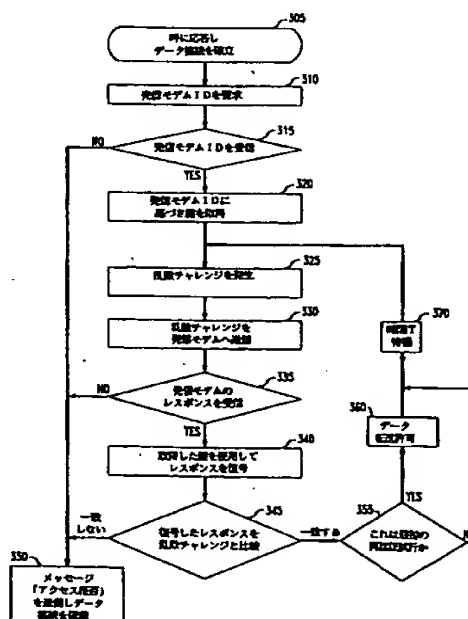
最終頁に続く

(54)【発明の名称】 データ通信装置およびデータ通信方法

(57)【要約】

【目的】 コンピュータ設備とユーザの間の公衆交換電話網(PSTN)のモデム間の再認証手続きによって、侵入者によるアクティブ傍受に対してコンピュータ設備を保護する安全な方法を提供する。

【構成】 ユーザのモデムとコンピュータのモデムは、データ接続期間中再認証手続きを実行する。この再認証手続きはデータ接続のサイドチャンネルで透過的に実行される。このサイドチャンネルは帯域内チャンネルでも帯域外チャンネルでもよい。再認証手続きは、2つのモデム間での暗号化された情報の交換からなる。一方のモデムがアクティブ傍受の存在を検出すると、モデムは単にデータ接続を中断する。



【特許請求の範囲】

【請求項1】 他のデータ通信装置へ複数のチャレンジを送信し、そのデータ通信装置からその複数のチャレンジのそれぞれに対応する複数のレスポンスを受信する送受信手段と、

各レスポンスの確認を表す出力を生成するために、各チャレンジの関数として各レスポンスを確認する手段とからなり、

その確認によって、出力が、レスポンスのうちの1つが確認されないことを表している場合にデータ接続を中断することを特徴とする、データ接続のユーザを再認証するデータ通信装置。

【請求項2】 前記確認手段が、前記他のデータ通信装置の識別子の関数でもあることを特徴とする請求項1の装置。

【請求項3】 前記送受信手段が、前記他のデータ通信装置に識別情報の要求を送信し、前記他のデータ通信装置からその識別子を受信することを特徴とする請求項2の装置。

【請求項4】 前記確認手段が複数の復号されたレスポンスを生成し、そのそれぞれは、前記他のデータ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数であり、前記確認手段が、復号された各レスポンスを、各チャレンジと比較して確認を表す出力を生成し、それによって、チャレンジと、復号されたレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項3の装置。

【請求項5】 前記確認手段が各チャレンジを暗号化し、その暗号化は、前記他のデータ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数であり、前記確認手段が、各レスポンスを、暗号化された各チャレンジと比較して確認を表す出力を生成し、それによって、暗号化されたチャレンジとレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項3の装置。

【請求項6】 前記確認手段が対称データ暗号化アルゴリズムの関数であることを特徴とする請求項1の装置。

【請求項7】 前記確認手段が非対称データ暗号化アルゴリズムの関数であることを特徴とする請求項1の装置。

【請求項8】 各チャレンジが乱数であり、前記データ通信装置がモデムであることを特徴とする請求項1の装置。

【請求項9】 第1のデータ通信装置とユーザの第2のデータ通信装置からなるデータ接続において、第1データ通信装置で使用するための、ユーザを再認証するデータ通信方法において、

第2データ通信装置へ複数のチャレンジを送信し、そのデータ通信装置からその複数のチャレンジのそれぞれに対応する複数のレスポンスを受信する送受信ステップ

と、

各レスポンスの確認を表す出力を生成するために、各チャレンジの関数として各レスポンスを確認するステップとからなり、

その確認によって、出力が、レスポンスのうちの1つが確認されないことを表している場合にデータ接続を中断することを特徴とする、データ通信方法。

【請求項10】 前記確認ステップが、第2データ通信装置の識別子の関数でもあることを特徴とする請求項9の方法。

【請求項11】 前記送受信ステップが、第2データ通信装置に識別情報の要求を送信し、第2データ通信装置からその識別子を受信することを特徴とする請求項10の方法。

【請求項12】 前記確認ステップが、それぞれ、第2データ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数である複数の復号されたレスポンスを生成するステップと、

確認を表す出力を生成するために、復号された各レスポンスを各チャレンジと比較するステップとを有し、その比較によって、チャレンジと復号されたレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項11の方法。

【請求項13】 前記確認ステップが、第2データ通信装置の識別子の関数として選択されたデータ暗号化鍵の関数として各チャレンジを暗号化するステップと、

確認を表す出力を生成するために、各レスポンスを、暗号化された各チャレンジと比較するステップとを有し、その比較によって、暗号化されたチャレンジとレスポンスの間に不一致がある場合にデータ接続を中断することを特徴とする請求項11の方法。

【請求項14】 前記確認ステップが対称データ暗号化アルゴリズムの関数であることを特徴とする請求項9の方法。

【請求項15】 前記確認ステップが非対称データ暗号化アルゴリズムの関数であることを特徴とする請求項9の方法。

【請求項16】 各チャレンジが乱数であり、データ通信装置がモデムであることを特徴とする請求項9の方法。

【請求項17】 第1のデータ通信装置とユーザの第2のデータ通信装置からなるデータ接続においてユーザを再認証するデータ通信方法において、

a) それぞれデータ暗号化鍵に関係づけられた複数の識別番号からなる鍵リストを第1データ通信装置に格納するステップと、

b) 第1データ通信装置において第2データ通信装置から識別番号を受信するステップと、

c) 第2データ通信装置から受信した識別番号に関係づ

けられたデータ暗号化鍵を鍵リストから取得するステップと、

d) 第1データ通信装置から第2データ通信装置へ、番号からなるチャレンジを送信するステップと、

e) 第1データ通信装置において第2データ通信装置から、番号からなるレスポンスを受信するステップと、

f) 第1データ通信装置において、レスポンスの確認を表す出力を生成するために、第2データ通信装置からのレスポンスを、取得したデータ暗号化鍵の関数として処理し、その出力が、第2データ通信装置の識別子の確認を表している場合にステップd) からf) までを反復し、第2データ通信装置の識別子が確認されなかった場合にデータ接続を中断するステップとからなることを特徴とするデータ通信方法。

【請求項18】 ステップf) が、

復号されたレスポンスを生成するために、取得したデータ暗号化鍵の関数としてレスポンスを復号することによって第2データ通信装置からのレスポンスを処理するステップと、

復号されたレスポンスをステップd) のチャレンジと比較し、復号されたレスポンスがステップd) のチャレンジと等しい場合にステップd) からf) までを反復し、復号されたレスポンスがステップd) のチャレンジに等しくない場合にデータ接続を中断するステップとを有することを特徴とする請求項17の方法。

【請求項19】 ステップf) が、

暗号化されたチャレンジを生成するために、取得したデータ暗号化鍵の関数としてチャレンジを暗号化することによって第2データ通信装置からのレスポンスを処理するステップと、

レスポンスを暗号化されたチャレンジと比較し、レスポンスが暗号化されたチャレンジに等しい場合にステップd) からf) までを反復し、レスポンスが暗号化されたチャレンジに等しくない場合にデータ接続を中断するステップとを有することを特徴とする請求項17の方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、モデムおよびコンピュータシステムに関する。特に、本発明は、コンピュータシステムへの安全なアクセスを提供するモデムの使用に関する。

【0002】

【従来の技術】今日の世界におけるコンピュータの使用は、メインフレームからパーソナルコンピュータに至るまで、連続的に増加しており、ますます多くの人々がコンピュータシステムを使用しつつある。実際、コンピュータ自体へのアクセスが可能であることによって、ほとんどの人が、モデムおよび公衆交換電話網(PSTN)を通じて、コンピュータの使用から恩恵を受けることが可能になっている。残念ながら、このアクセス可能性

は、「侵入者」、すなわち、コンピュータシステムの違法ユーザを引き付けているようにも思われる。その結果、コンピュータに格納されている情報の正当性および分配に関する、コンピュータシステム、またさらにはコンピュータの網のセキュリティは、コンピュータの合法ユーザ、所有者、およびオペレータの関心の事項となっている。

【0003】ある種のアクセスセキュリティをコンピュータシステムに提供するこの必要性に回答して、アクセス要求ユーザの同一性を認証するためにさまざまな方法が使用されている。1つの例は、周知のとおり、「パスワード」の使用である。この変形として、モデムアクセスの場合、「パスワード/コールバック」方式がある。これは、ユーザによるパスワードの入力が成功した後、被呼コンピュータが所定の電話番号でユーザにコールバックするものである。もう1つの例は、チャレンジ/レスポンス方式である。これは、コンピュータ(付与者)が、乱数(チャレンジ)をユーザ(要求者)へ送信し、要求者は、付与者と要求者によって共有されている秘密の鍵(キー)を使用してその乱数を暗号化することによって、要求者の同一性を証明する、というものである。実際、「チャレンジ/レスポンス」プロトコルおよびデータ暗号化規格(DES)アルゴリズムを使用した強力なノード間認証手続きを提供する、ANSI X9.26-1990「卸売財務システム用開始認証」のような工業規格がある。

【0004】しかし、パスワードおよびパスワード/コールバック方式は、後でデータ接続を制御し、それによってコンピュータシステムを「欺く」者に対する保護を提供することはほとんどできない。さらに、ANSI X9.26-1990のチャレンジ/レスポンス法は、最初の開始(ログイン)手続き中にユーザの同一性を認証する方法を与えるのみである。換言すれば、上記の方法は、最初の開始手続き後にユーザを切断し、コンピュータにアクセスするためのデータ接続の侵入者による制御を可能にする「アクティブ傍受」を使用する侵入者に対する保護はしない。

【0005】その結果、コンピュータシステムへのアクセスセキュリティが、データ接続自体のプライバシーと比べて最重要事項である場合、データ接続がアクティブ傍受に侵されないことを保証する他の技術が要求される。例えば、DES暗号化を使用したデータストリームの完全な暗号化は、侵入者が後でアクセスすることを防ぐ1つの可能な手段である。もう1つの手段が、米国特許第4,802,217号(発明者:ミチェナー(Mitchener)、発行日:1989年1月31日)に記載されている。それによれば、コンピュータが、ユーザの端末とユーザのモデムの間に接続されたセキュリティデバイスを制御する。特に、ユーザは、コンピュータシステムにダイヤルし、コンピュータシステムはセキュリ

ティデバイスから暗号化された第1の符号語を受信する。続いて、コンピュータは、セキュリティデバイスに対し、この第1暗号化符号語を第2の暗号化された符号語に変更するよう命令し、ラインを切断し、ユーザにコールバックする。コンピュータによるコールバックが完了すると、セキュリティデバイスは、データ接続を確立するために、第2暗号化符号語をコンピュータに送信する。その後、コンピュータは、セキュリティデバイスに対し、定期的に、他の暗号化符号語に変更するよう命令し、そのたびに、セキュリティデバイスは、新たに暗号化された符号語をコンピュータに送信し、それに対してコンピュータは受信した暗号化符号語をチェックし、それによって、もとのユーザへのデータ接続の正当性の継続を確認する。

【0006】

【発明が解決しようとする課題】結果として、完全なデータ暗号化によって、または、ミチエナー特許によって提案されたように、定期的再認証によって、同一性の一定の再確認がなければ、侵入者はラインを橋絡し、データ接続を引き継ぎ、それによって、リソースおよび情報への無許可のアクセスを取得し、有利になるように情報を注入することができる。しかし、この従来技術は、アクティブ傍受に対するあるレベルの保護は提供するが、問題に対する完全な解答ではない。例えば、完全なデータ暗号化は、一般にコンピュータおよびユーザの端末に関して、コンピュータシステムのコストおよび複雑さの両方に影響する。同様に、ミチエナー特許は、コンピュータソフトウェアの修正、および、ユーザの端末とユーザのモデム間の別個のセキュリティデバイスを必要とする。

【0007】

【課題を解決するための手段】本発明は、コンピュータのユーザ、所有者、およびオペレータに、コンピュータへのPSTNデータ接続のアクティブ傍受に対するアクセスセキュリティを提供する際の柔軟性を提供する。特に、われわれの認識では、PSTNデータ接続において一般的に共通の要素の1つは、端末機器と伝送媒体の間を媒介する機器、すなわち、モデムである。従って、本発明の原理によれば、モデム間の連続的再認証手続きによってアクセスセキュリティがPSTNデータ接続に与えられる。この連続的再認証手続きは、データ接続期間中に認証情報を定期的または非定期的に送信するために、データ接続のサイドチャネルを使用することによって、非干渉的に行われる。このサイドチャネルは、帯域内でもよい。この場合、再認証情報はデータ伝送間に時分割多重化される。または、サイドチャネルは帯域外でもよい。この場合、利用可能帯域幅の狭い部分が、周波数分割多重(FDM)方式を使用して再認証情報を交換するために使用される。その結果、アクセスセキュリティがPSTNデータ接続に透過的に提供され、追加のセ

キュリティデバイスやユーザの機器またはコンピュータシステムへの修正は不要となる。

【0008】本発明の一実施例では、着信モデムおよび発信モデムの両方がDESアルゴリズムをサポートし、着信モデムは発信モデムを再認証する。発信モデムを再認証するため、着信モデムは、データ接続期間中ときどきチャレンジ/レスポンスシーケンスを発信する。特に、着信モデムは、データ暗号化鍵のリストを有し、各データ暗号化鍵は、特定モデムの識別子に対応する。電話呼に応答すると、着信モデムは、発信モデムに対し、対応するデータ暗号化鍵を選択することができるように、識別子を送信することによって、自分自身を識別するよう要求する。その後、着信モデムは、ときどき、発信モデムにチャレンジとして送信される乱数を発生する。発信モデムは、チャレンジを受信すると、着信モデムにレスポンスを返す。このレスポンスは、乱数の暗号化された形式である。発信モデムの暗号化プロセスは、着信モデムによって使用されたデータ暗号化鍵と同一のデータ暗号化鍵を使用する。着信モデムは、そのレスポンスを復号し、それをチャレンジと比較する。復号したレスポンスとチャレンジが一致した場合、発信モデムの同一性が確認される。しかし、復号したレスポンスとチャレンジが一致しない場合、詐欺の可能性のある試行が検出されたことを示し、着信モデムはデータ接続を単に破棄する。

【0009】

【実施例】図1に、二地点間データ通信システムを示す。以下の例では、端末110の発呼者(ユーザ)が、発信モデム120、電話網130、および着信モデム200を通じて被呼者(コンピュータ150)にアクセスするために、電話呼を発信すると仮定する。ライン201および121は、電話網130によって提供される一般的な「チップ/リング」、すなわちローカルループのアクセスを表す。モデム120および200の両方が本発明の原理を実現するが、簡単のためモデム200のみ詳細を図2に示す。以下で説明する本発明の概念を除いて、モデム200は、従来周知のデータ通信機器(DCE)を表し、データ端末機器(例えばコンピュータ150)とデータ回線(ここではPSTN)をインタフェースする。PSTNはライン201および121、ならびに電話網130によって表される。特に、本発明の説明では、データ通信機器という用語は、1)データ接続を確立するのに必要な機能、ならびに2)データ端末機器とデータ回線の間の信号変換および符号化を提供する装置を意味する。モデム200は、メモリ220、CPU210、デジタル信号プロセッサ(DSP)250、データ暗号化プロセッサ230、データ通信インタフェース260、およびデータ端末インタフェース240からなる。CPU210はマイクロプロセッサ中央処理装置であり、バス211を通じてメモリ220に格納され

たプログラムデータに作用し、またはそれを実行する。メモリ220はランダムアクセスメモリを表し、いくつかの代表的な記憶ロケーションを有し、そのサブセットが図2に示されている。メモリ220は、鍵リスト221を有すると仮定する。データ暗号化プロセッサ230はDES暗号化規格をサポートし、リード213を通じてCPU210によって供給されるデータに作用する。例えば、データ暗号化プロセッサ230は、DES規格（例えば「連邦情報処理規格46」）によって指定される「電子コードブック暗号化」プロセスに従って作用する。注意すべきことであるが、明確化のため、データ暗号化プロセッサ230はCPU210およびメモリ220とは別に図示されている。しかし、以下の説明から明らかになるように、もう1つの、より安価な実現は、データ暗号化プロセッサ230によって実行されるデータ暗号化アルゴリズムが単にCPU210によって直接実行され、その場合CPU210はメモリ220に格納されたデータ暗号化プログラムを実行するというものである。最後に、簡単のため、DSP250は、入力または出力信号を処理するための、フィルタ、アナログーデジタル変換器およびデジタルーアナログ変換器のような他の周知の処理機能を有すると仮定する。

【0010】モデム120からの発信電話呼の結果、モデム200は電話網130からリード201によって入力信号を受信する。この入力信号は、データ通信インタフェース260によってDSP250に送られる。DSP250は、CPU210の制御下で、CCITT V.32呼確立シーケンスを実行する。このシーケンスは、モデム120とのデータ接続を確立するためのモデムハンドシェイクおよびトレーニングを含む。データ接続の確立後、DSP250は、コンピュータ150（データ端末インタフェース240を通じて）と端末110（データ通信インタフェース260を通じて）との間で生じるデータストリームの信号変換および符号化を実行する。

【0011】本発明の原理によれば、着信モデム200は、チャレンジ/レスポンスプロトコルによって、発信モデム120のユーザ透過的（暗号）一方向ノード間再認証を実行する。その流れ図を図3に示す。特に、ステップ305で、発信モデム120とのデータ接続を確立した後、CPU210はステップ310に進み、DSP250を通じてモデム識別（ID）番号をモデム120に要求する。モデムID番号とは、発信モデムに割り当てられた所定の番号である（後述）。ステップ315で、CPU210が、発信モデムのID番号を受信しない場合、ステップ350で、CPU210は単にメッセージ「アクセス拒否」を送信し、データ接続を破棄する。一方、CPU210が発信モデムのID番号を受信した場合、CPU210はステップ320に進み、鍵リスト221から対応するデータ暗号化鍵を取得する。鍵

リスト221は、事前にメモリ220に格納されており、複数のモデムID番号を表す。各モデムID番号はそれぞれ可能な発信モデムを表し、データ暗号化鍵に関係づけられている。この関係づけられたデータ暗号化鍵もまた、モデムIDと同様に、発信モデムにおいて事前に決定されている。

【0012】モデム120のデータ暗号化鍵を取得した後、ステップ325で、CPU210は乱数を発生する。これはチャレンジとして知られる。ステップ330で、このチャレンジはモデム120に送信される。モデムからチャレンジを受信すると、モデム120は、データ暗号化プロセッサ（図示せず）によってそのチャレンジを暗号化し、レスポンス（すなわち、ある形式の「暗号文」）を発生し、モデム200に返送する。モデム120によって実行される暗号化は、上記の格納されているデータ暗号化鍵を使用する。チャレンジおよびレスポンスはそれぞれ少なくとも20ビットのデータからなるため、正しいレスポンスを発見する可能性は100万分の1しかない。ステップ335で、CPU210がモデム120からレスポンスを受信しない場合、ステップ350で、CPU210はメッセージ「アクセス拒否」を送信し、データ接続を破棄する。一方、CPU210がレスポンスを受信した場合、CPU210はステップ340に進み、ステップ320で取得したデータ暗号化鍵を使用してその応答を復号する。受信したレスポンスの復号は、DES暗号化規格をサポートするデータ暗号化プロセッサ230を介してCPU210によって実行される。続いてCPU210はモデム120の同一性を確認する。ステップ345で、復号したレスポンスとチャレンジが一致しない場合、ステップ350で、CPU210はメッセージ「アクセス拒否」を送信し、データ接続を中断（例えば破棄）する。（この時点で、着信モデム200には別の選択肢があることに注意すべきである。例えば、データ接続を破棄する代わりに、データ接続の「トレース」を開始することができる。）一方、CPU210が、モデム120の同一性を確認した場合、すなわち、復号したレスポンスとチャレンジが一致した場合、CPU210はデータ接続を妨害せずにステップ355に進み、これが最初の再認証試行の完了であるかどうかをチェックする。これが最初の再認証試行の完了である場合、ステップ360で、CPU210は、モデム200とモデム120の間のデータ情報の転送を可能にする。いったんデータ転送が可能となると、後の再認証試行はステップ360をバイパスして直接ステップ370にすみ、CPU210は所定時間Tの割り込みをセットする。時間Tの経過後、CPU210は、ステップ325〜345を反復することによって、データ接続を再認証する。この再認証プロセスは、データ接続期間中継続される。

【0013】上記の認証プロセスを図4にも示す。着信

モデム300(付与者)は、「モデムID送信」メッセージ605を発信モデム120(要求者)に送信し、発信モデム120は「ID」610を送信することによって応答する。その後、着信モデム200は「チャレンジ」615を発信モデム120に送信し、発信モデム120は、「レスポンス」620を送信する。レスポンス620の復号が、上記のように、チャレンジ615と一致した場合、着信モデム200は「OK」メッセージ625を送信することができる。一方、レスポンス620の復号がチャレンジ615と一致しない場合、モデム200は「アクセス拒否」メッセージ630を送信する。

【0014】上記の図3以外のもう1つの方法を図5に示す。相違点はステップ540および545のみである。ステップ540で、モデム200は、ステップ330でモデム120に送信したチャレンジを暗号化する。このチャレンジは、ステップ320で取得したモデム120に関係づけられたデータ暗号化鍵を使用して暗号化される。モデム120の同一性の確認は、ステップ545で、暗号化したチャレンジとモデム120からのレスポンスとを比較することによって実行される。上記のように、モデム120によって暗号化されたチャレンジ(すなわち、レスポンス)が、モデム200によって暗号化されたチャレンジと一致した場合、データ接続は妨害されず、CPU210はステップ355に進む。しかし、一致しない場合、ステップ350で、データ接続は中断される。

【0015】上記の図3および5の再認証プロセスは、データ接続のサイドチャンネルで実行される。換言すれば、データ接続の帯域幅の一部が再認証情報を伝送するために使用される。その結果、データ接続は、基本チャンネル(データ伝送用)およびサイドチャンネル(補助的情報伝送用)からなる。このサイドチャンネルは、基本的に、再認証情報をデータの伝送と多重化する。特に、サイドチャンネルでは、帯域内チャンネルまたは帯域外チャンネルが使用される。

【0016】帯域外サイドチャンネルの例は、データと再認証情報の周波数分割多重化(FDM)をするものである。この形式の帯域外チャンネルは「二次チャンネル」としても知られており、一般的に、低ビットレートチャンネル専用の、周波数スペクトルの狭い部分である。周波数スペクトルの例を図6に示す。データ接続は、帯域幅 f_w を有し、データ情報を伝送する基本チャンネル410と、帯域幅 f_n を有し、再認証情報を伝送する補助(狭帯域)チャンネル405からなると仮定している。

【0017】帯域内サイドチャンネルの例は、データと再認証情報の時分割多重化をするものである。これを図7に示す。モデム200とモデム120間でのデータの伝送の実際の構造は、下位のモデムプロトコル(例えばCCITT V.42の改訂版)を利用すると仮定する。このプロトコルは、データの伝送用の「データフレー

ム」と、制御(補助)情報の伝送用の「制御フレーム」とからなるHDL型のプロトコルである。図7に示すように、データフレーム(例えばデータフレーム510)は、制御フレーム(例えば制御フレーム505)と時分割多重化されている。再認証情報は、制御フレーム505内で周知技術を使用してモデム200と120の間で単に伝送される。

【0018】上記のように、発信モデムと着信モデムは、再認証プロセス中、同一のデータ暗号化鍵を共有する。これは、「対称」データ暗号化として知られている。結果として、両方のモデムは同一のデータ暗号化鍵情報を格納していなければならない。さらに、少なくとも発信モデムはそのモデムIDを格納していなければならない。最後に、一方または両方のモデムは、上記の鍵リストを保持する。このリストは、可能な発信モデムIDのリストを、識別されるモデムに格納されているデータ暗号化鍵と同一のデータ暗号化鍵にそれぞれ関係づける。これらの情報はすべて、モデムパラメータの管理のための従来技術を使用して事前に初期化される。例えば、この情報は、モデムに接続された端末を通じて入力することも、「ダウンロード」方式を使用することによって遠隔で初期化することも可能である。

【0019】上記の反復再認証プロトコルは、チャレンジ/レスポンスプロトコルを例示しているが、他の再認証プロトコルも可能である。例えば、上記の方法よりは安全ではないが、モデム120および200は単純なパスワード方式を使用することができる。この場合、各モデムは同一のパスワードのリストを有し、各パスワードには番号が関係づけられる。この方式では、モデム200によって送信されるチャレンジは単にパスワードに関係づけられた番号である。モデム120によるレスポンスは単にその番号(チャレンジ)に割り当てられたパスワードである。モデム200は、モデム120の認証を判定するために、受信したパスワード(レスポンス)を、パスワードのリストに示された正確なパスワードと比較する。

【0020】もう1つの例は、上記の対称データ暗号化チャレンジ/レスポンスプロトコルと同様に安全なものであるが、「公開鍵」方式の使用である。これは、米国規格技術協会(NIST)によって開発され現在提案されている「デジタル署名規格」のような「非対称」形式のデータ暗号化である。公開鍵方式は、暗号化と復号に異なる鍵が使用されるため、非対称である。さらに、一方の鍵は秘密に保持される。他方の鍵は公開してよい。特に、モデム200は、上記のように、モデム120へチャレンジを送信する。しかし、モデム120は、「デジタル署名」および「証明書」を添付してそのチャレンジを返す。デジタル署名とは、チャレンジおよびモデム120の秘密のデータ暗号化鍵の関数であるデジタルビットパターンであって、モデム200には未

知である。証明書は、周知のように、モデム120からの識別情報および公開鍵を含む。この方法では、「要求者」が常に公開鍵を提供するため、モデム200はモデム識別子およびデータ暗号化鍵のリストを保持する必要はない。

【0021】以上、本発明の実施例を説明したが、本発明の原理に基づいてさまざまな変形例が可能である。例えば、上記の連続的再認証プロセスはモデム間データ接続に関して説明したが、他の形式のデータ通信機器（例えば端末アダプタ）もこの連続的再認証を実行すること

が可能である。

【0022】さらに、再認証は連続的であるが、再認証試行間の時間遅延Tは周期的である必要はなく、データ接続期間中「非周期的」、すなわち可変とすることが可能である。さらに、他の形式のサイドチャネル（例えば、基本信号点コンステレーションの変調）が可能である。また、上記では発信モデムのIDはハンドシェイクプロセスの後に受信したが、モデム識別情報の受信はハンドシェイクプロセス中に行うことも可能である。

【0023】また、上記の例では、暗号化を使用した一方向チャレンジ/レスポンス認証について説明したが、任意の種類の認証プロトコル（例えば、双方向のノード間再認証プロトコル）が、通信エンティティの識別子を認証するために使用可能である。例えば、双方向再認証プロトコルを実現するには、発信モデムは上記（図3）の着信モデムと同様のステップを実行する。特に、発信モデムもまた、着信モデムに自分自身を識別するよう要求し、その後、発信モデムは、着信モデムによって正確に暗号化されなければならないチャレンジを発行する。着信モデムの復号されたレスポンスが発信モデムのチャレンジと一致しない場合、発信モデムはデータ接続を中断する。

【0024】

【発明の効果】以上述べたごとく、本発明によれば、コンピュータ設備とユーザの間の公衆交換電話網のモデム

間の再認証手続きによって、侵入者によるアクティブ傍受に対してコンピュータ設備を保護する安全な方法が実現される。

【図面の簡単な説明】

【図1】二地点間データ通信システムのブロック図である。

【図2】図1のデータ通信システムで使用される本発明の原理を使用したモデムのブロック図である。

【図3】図2のモデムで使用される方法の流れ図である。

【図4】本発明の原理を使用する再認証手続きの流れ図である。

【図5】図2のモデムで使用されるもう1つの方法の流れ図である。

【図6】図2のモデムで使用される帯域外サイドチャネルの図である。

【図7】図2のモデムで使用される帯域内サイドチャネルの図である。

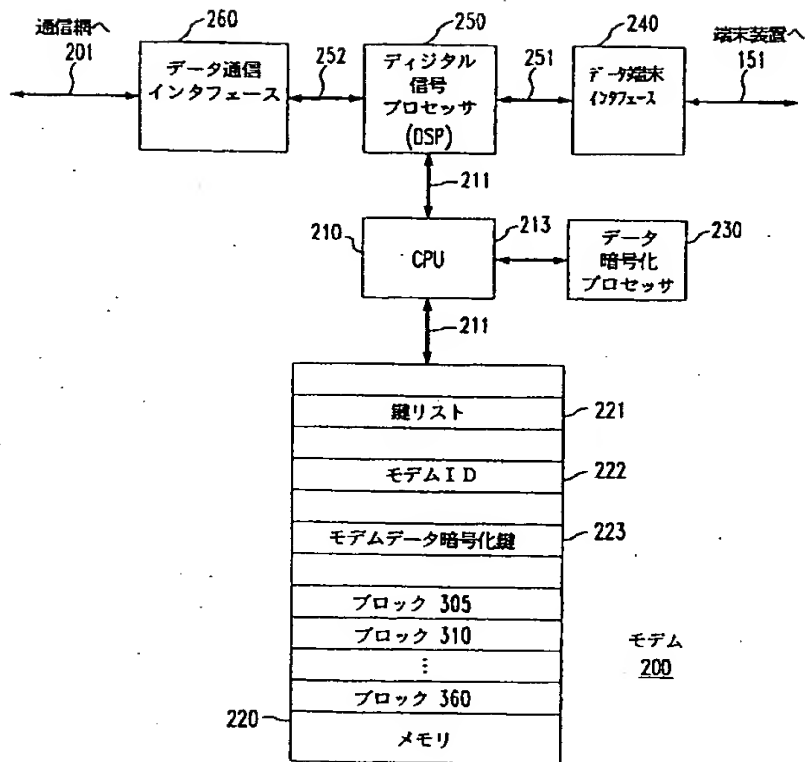
【符号の説明】

110	端末
120	発信モデム
130	電話網
150	コンピュータ
200	着信モデム
210	CPU
220	メモリ
221	鍵リスト
230	データ暗号化プロセッサ
240	データ端末インタフェース
250	デジタル信号プロセッサ (DSP)
260	データ通信インタフェース
405	補助 (狭帯域) チャネル
410	基本チャネル
505	制御フレーム
510	データフレーム

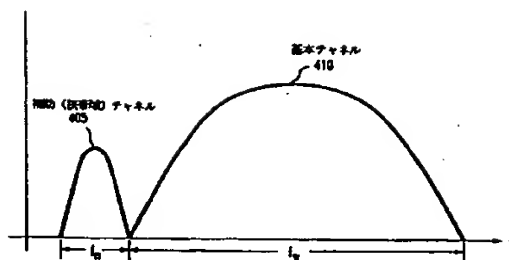
【図1】



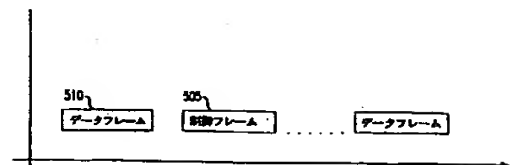
【図2】



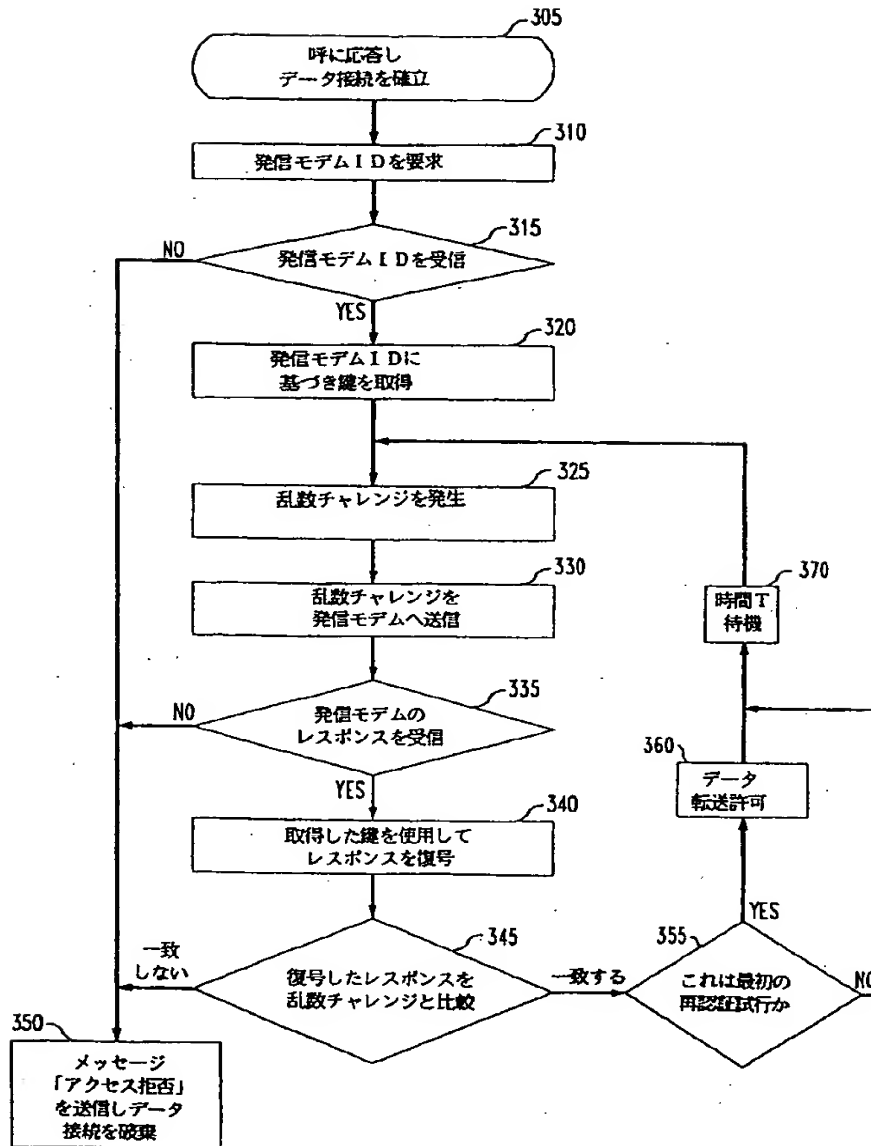
【図6】



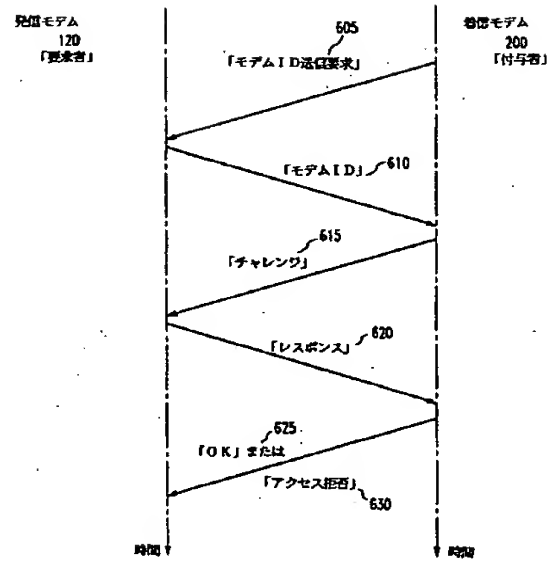
【図7】



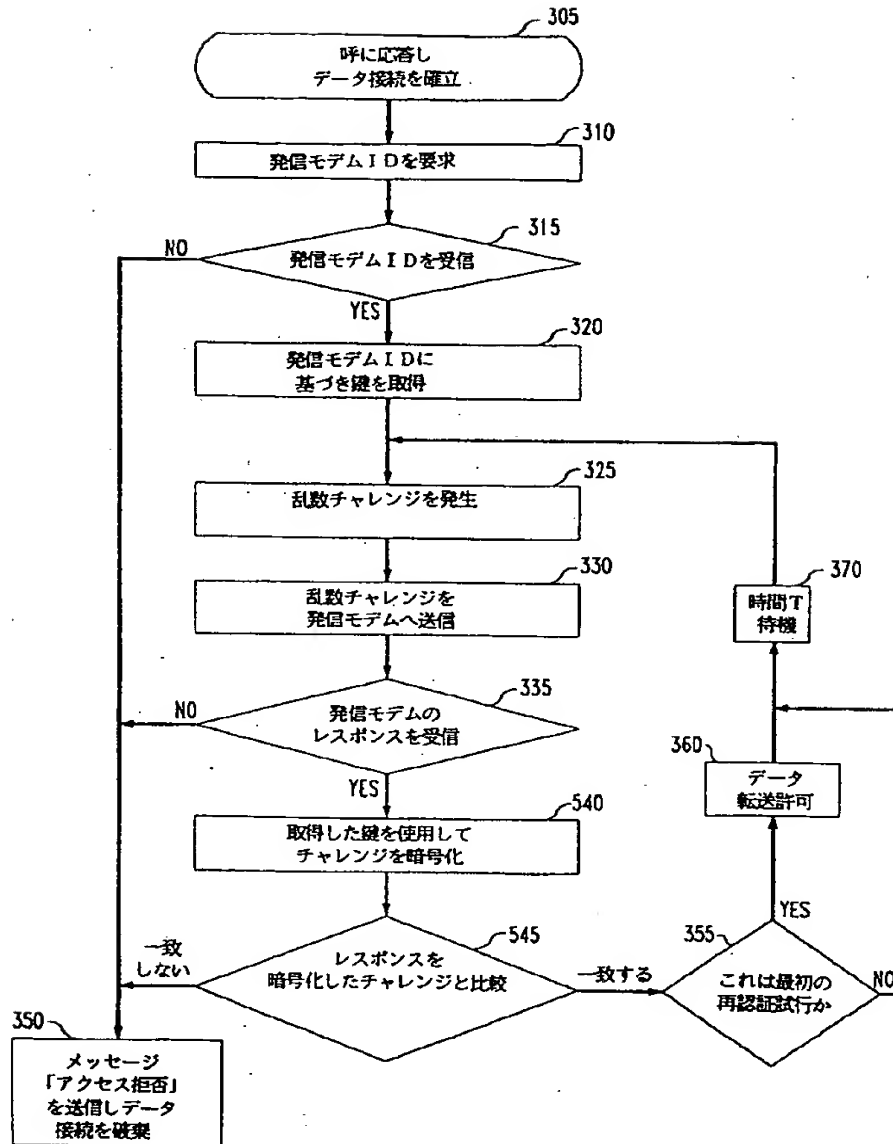
【図3】



【図4】



【図5】



フロントページの続き

(51) Int. Cl. 5

H 0 4 L 12/22

H 0 4 M 11/00

識別記号

3 0 3

庁内整理番号

7470-5K

F I

技術表示箇所

(72)発明者 ロバート アール スコット
アメリカ合衆国 34630 フロリダ クリ
アウォーター、ナンパ204、パイウェイ
ブルヴァード 640

(72)発明者 リチャード ケント スミス
アメリカ合衆国 34646 フロリダ セミ
ノール、アルパイン アヴェニュー
13471